防止を超えた対応策へ：次世代エンドポイント セキュリティが必要な理由

セキュリティ戦略を進化させて変化する脅威に対応

脅威は変化しています。今こそエンドポイント セキュリティ戦略も同じように変化させるべきときです。

数十年にわたり、組織はウイルス対策製品でマルウェアを防いできました。従来のアプローチは、既知のマルウェアを締め出すことによって組織のネットワークの境界を保護することを目的としていました。ウイルス対策製品は、ファイルがネットワークに入ろうとしたときにスキャンを行い、正常なものか悪意のあるものかを判断したうえで、分析結果に基づいてそれらをブロックするのか、またはネットワークを通過させるのかを決定していました。当時、これらのツールは効果的で目的にかなっていましたが、脅威の状況とサイバーセキュリティ チームの進化に伴って、防止策だけでは対応できなくなりました。

より高度な回避技術

組織が数十年をかけて従来のマルウェア防止ツールの仕組みを理解する一方、攻撃者も同様にそれを理解してきました。その結果、マルウェア作成者は自らを隠して検出を回避できるマルウェアの設計に関して、非常に高いスキルを身に付けました。特定タイプのマルウェアの成功率が低下すると、攻撃者は新たな変種を作成します。攻撃者のアプローチは動的で、静的なポイントインタイム ツールでは対応できない速度で変化します。このような動的な攻撃者に打ち勝つことができるソリューションを構築するには、これらの攻撃がどのように動作するのか、そしてどのような回避技術が攻撃を成功へと導いているのかを理解する必要があります。

目次

今日の一般的な回避技術には、以下のようなものがあります。

環境認識型のマルウェア

この技術は、仮想マシンまたはサンドボックス環境内でマルウェアが実行されている形跡がないかどうかを探り、その動作を変化させて分析を回避します。これには、スキャンされるまでファイルを待機させて悪意のある動作を実行する遅延戦術が含まれます。別の戦術ではユーザの操作が必要とされ、エンド ユーザがマウスを一定数クリックするか動かす、または特定のプログラムを起動するまでファイルを待機させて、悪意のある動作を顕現させます。

ルアー ドキュメント

ルアー ドキュメントは厳密には無害なものですが、多くの場合、悪意のあるマクロやマルウェアが組み込まれたドキュメントへと誘導する URL リンクを含んでいます。エンド ユーザは一般的に、非常に説得力がある標的型のフィッシング メールを通じてこうしたドキュメントを受け取ります。

ドメイン生成アルゴリズム（DGA）

マルウェアを常に新しく有効な状態に保つために、攻撃者はアルゴリズムを使用してさまざまなドメイン名を作成することで、トラフィックを隠し、検出を回避します。つまり、非常に多くのドメイン名を生成することで、そのすべてをブロックできないようにすることがその目的です。DGA は一般的に存続期間の短いものでしたが、その平均期間は大幅に延び、現在では最大約 40 日となっています。

ファイルレス マルウェア

このタイプのマルウェアは、ファイル システムまたはレジストリに一切アーティファクトを書き込むことなく、メモリ内で完全に動作します。つまり攻撃者が、被害者を再感染させるためのコマンドをレジストリに保存するといった永続的なメカニズムの導入を望まない限り、書き込む必要はありません。システムの起動時に自動的にコマンドが実行されます。ファイルレス マルウェアは他のマルウェアより検出が難しく、システムの永続的な変更が最小限に抑えられるか完全に回避されるため、フォレンジック調査やインシデント対応はさらに困難になります。

ポリモーフィック型

この技術により、マルウェア サンプルは自らを変化させて特定のファイル、またはファイル内のパターンを探すシステムを回避できます。マルウェアは、コードの特定の部分を保存する場所を変えたり、さまざまな方法で自らの一部をエンコーディングまたは暗号化したり、特定の値を変えるか一部を追加または削除することによって自らの重要ではない部分を変更したりなど、多様な方法でこれを実現することが可能です。

ピギーバック

これは、マルウェアの作成者が、求められているソフトウェアとともに通常は不必要なソフトウェアを追加でインストールする方法です。ソフトウェアの作成者側からすると、ソフトウェアをバンドルする機能は正当で意図したものかもしれませんが、悪意のある攻撃者は、サプライ チェーン攻撃として知られる手法を通じてユーザにマルウェアを仕掛けることができます。このシナリオでは、攻撃者が正当なソフトウェアの開発またはリリース プロセスの一部を制御し、ソフトウェアの作成者やユーザに気付かれることなく、プロセス内に悪意のあるコードをバンドルすることが可能です。

業界の対応

業界で新しい脅威の種類または回避技術が発見されるとすぐに、最新の製品の販売を促進する機会として捉えられます。その製品は、次の新たな脅威が登場してさらに別のツールが必要になるまで、しばらくは役に立ちます。その結果、組織は包括的なソリューションに投資するのではなく、最新の保護手法ばかりに重点を置いた製品を実装するサイクルに陥ってきました。数年先には、互いに連携しないエンドポイント セキュリティ ツールが組織内にあふれることとなり、高いスキルを持った、見つけることが難しい多数の IT スタッフによる管理が求められるようになるうえ、必要な資金が増え続け、その調達がより一層困難になる可能性があります。

何が必要なのか：全面的な変革

では、どのようにすれば組織はこのサイクルから抜け出し、より効果的かつ効率的に高度な脅威から自らを守ることができるようになるのでしょうか。ここで必要となるのは、悪意のあるアクティビティの検出方法を全面的に変革することです。防御者には、従来のポイントインタイム技術にあるような制約がない統合ソリューション、つまり次世代のエンドポイント セキュリティが必要です。

次世代エンドポイント セキュリティ（NGES）とは、本質的に統合ソリューションの形で保護、検出、および応答機能を提供する複数の技術の集まりです。このモデルでは、検出と応答がもはや個別の領域やプロセスではなく、密接した継続的なアプローチの延長線上にあります。これらのコンポーネントが単一の統合システムに集約されると、組織においてエンドポイント セキュリティの効率と効果が高まり始めます。

次世代エンドポイント セキュリティの機能には、以下のようなものがあります。

継続的な検出と可視性

大部分の潜在的脅威の排除において、防止は引き続き重要な役割を果たしますが、防止機能だけに頼るのではなく、それらをソリューションの一部とみなすことが大切です。最初の防止フェーズの後に継続的な検出が可能な技術を適用すれば、高度なマルウェアを阻止するための取り組みが、より効果的かつ効率的なものとなります。継続的アプローチは、次世代エンドポイントモデルの基盤であり、さらなるイノベーションを促進します。

次世代のイノベーション	
レトロスペクティブな検出	マルウェアの侵入後にファイルを継続的に追跡および監視することにより、最初の検出を回避した悪意のあるアクティビティを検出して修復できます。
ファイル トラジェクトリ	0 号患者を特定し、環境全体で長時間にわたってファイルの伝播を監視することにより、可視性を向上させるとともに、マルウェア侵害の範囲を詳しく調べるのに必要な時間を短縮できます。
柔軟な検索	ファイルのテレメトリおよび集合型セキュリティ インテリジェンス データにわたる制限のない検索を使用して、侵害の状況と範囲を迅速に把握し、侵害の兆候や悪意のあるアプリケーションを見極めることができます。
デバイス トラジェクトリ	侵害が起きる前後のイベントの履歴を迅速に把握し、脆弱なアプリケーションを特定できます。

次世代のイノベーション	
拡散度	ごく一部のホストだけに存在する実行ファイルを特定することにより、これまでに検出されず少数のユーザが目撃した脅威を明らかにできます。これにより、検出されなければより広範なネットワークに侵入する可能性がある高度で永続的な標的型攻撃が特定されます。
アウトブレイク コントロール	コンテンツの更新を待つことなく、疑わしいファイルや脅威の拡大を制御し、感染を修復できます。

高度な分析

ネットワークを横方向に移動してエンドポイント全体に広がる攻撃を検出するために、防御者には侵害の兆候（IoC）を自動的に探すソリューションが必要です。また、これらのソリューションは、インシデントを示すより微小で高度な動作を見つけ出すものでなければなりません。ビッグデータ分析と継続的な機能を使用することにより、セキュリティ チームは発生と同時にパターンや IoC を特定し、損害をもたらす可能性が最も高い脅威への対応に注力できます。

情報に基づく調査

コンテキストや継続的アプローチの機能がなければ、コンテキストに関する証拠がほとんどない状態で調査を進め、侵害を追跡するという大変な作業が必要になります。多くの場合、どこから始めればよいのかが最も難しい課題の 1 つとなりますが、次世代ソリューションを活用すれば、より迅速かつ生産的に的を絞った調査を行うことが可能になります。セキュリティ チームは、感染の侵入ポイント、範囲、および根本原因をより的確に把握し、実際のイベントに基づいて焦点を定めた侵害の調査を開始できます。

効率的な封じ込め

感染している可能性があるすべてのエンドポイントのイメージ変更が必要とされる場合、マルウェアの封じ込めは非常に困難になることがあります。ポイントインタイム技術ではイベントの連鎖やそれに伴うコンテキスト情報を見つけることができず、またマルウェアを外科的に封じ込める機能は現実的ではありません。可視性を向上させるとともに、特定の根本原因に焦点を当てる機能を使用すれば、迅速かつ容易に脅威の拡大を阻止することが可能になります。検出およびテレメトリ データを保存することにより、攻撃経路のさまざまなポイントで脅威を封じ込め、最初の感染の侵入口を閉じて将来の攻撃を阻止できます。

関連性レポート

会議室でセキュリティに関する議論が交わされることが増えつつある中、ビジネスとの関連性や起こり得るリスクを明らかにする実用的なダッシュボードや動向をレポートに含めることにより、こうした議論を活性化させる必要があります。ポイントインタイム技術でも、ダッシュボードおよびリスクの関連性を提供できますが、一般的には、大量のイベント データを厳密に調査して関連付けるために、さらなる製品の統合が必要となります。次世代のレポート機能は、データを使用して組織が最も必要としているタイミングと場所でコンテキストを提供し、優先順位付けを行います。

統合セキュリティ アーキテクチャの重要性

これらのイノベーションはどれも同じくらい重要なものですが、統合されたワークフローでこれらを組み合わせて使用すると、マルウェアの検出、監視、分析、調査、および封じ込めの効果が大きく高まります。

ネットワーク全体で他のセキュリティ ツールと脅威インテリジェンスを共有し、それを関連付けることが可能なエンドポイント ソリューションは、セキュリティ チームの力を増強させます。エンドポイント ツールとルータ、ネットワーク IPS、ファイアウォール、Web プロキシ、および E メール ゲートウェイを統合すれば、包括的な対応が可能なセキュリティ エコシステムが構築されます。完全に統合されたセキュリティ アーキテクチャなら、より迅速かつ包括的な保護が可能です。

まとめ

今日の高度な脅威に効果的に対処するために、組織には高度な可視性、コンテキスト、および制御で侵害を阻止するソリューションが必要です。さらに、マルウェアが侵入した場合、こうしたソリューションはマルウェアを迅速に検出して封じ込め、修復できるものでなければなりません。エンドポイント セキュリティに対する継続的アプローチは、エンドポイントを標的とする高度な脅威に対処できる重要なイノベーション領域の実現に貢献します。これには、以下のようなものが含まれます。

継続的な監視と分析

継続的アプローチでは、検出がより効果的、効率的、かつ包括的に行われます。このアプローチは、サンドボクシングのような動作検出手法を最適化するとともに、明らかになったアクティビティをキャプチャし、検出エンジンと制御ポイント全体でインテリジェンスを共有します。

長期間にわたって動作を監視する自動化された高度な分析

セキュリティにおいて高度な分析と継続的な機能を使用し、発生と同時にパターンや IoC を特定すれば、最も重要な脅威への対応に注力できます。

狙われる側から狙う側へと変える調査

調査から、実際のイベントと IoC に基づいて脅威を探す焦点を絞った捜索に切り替えることで、セキュリティ チームは攻撃の範囲を素早く、効果的に把握することができます。

きわめてシンプルな封じ込め

継続的アプローチが提供する可視性レベルと、特定の根本原因に焦点を当てる機能を組み合わせることで、攻撃チェーンを素早く効果的に壊すことができます。

実用的なコンテキストに基づくダッシュボード

これらのダッシュボードにより、制御ポイント全体にわたるファイルおよびテレメトリ データの包括的な収集と高度な分析の状況が報告されます。その後、ダッシュボードでこれらにコンテキスト情報が重ねられ、動向、ビジネスとの関連性、およびリスクに対する効果が明らかにされます。

Cisco® Advanced Malware Protection（AMP）for Endpoints は、次世代エンドポイント セキュリティを提供します。これによって組織は、今日の高度な脅威から自らを保護することが可能になります。

次世代エンドポイント セキュリティの効果をご自身の目で確かめたいとお考えのお客様は、今すぐ 4 週間ご利用いただける無償試用版をお申し込みください。

C11-740006-00　12/17